**Framework in Focus – Matthew McCollough**

**Mr. Petersen:** Welcome to the NICE eNewsletter regular column on the NICE Cybersecurity Workforce Framework in Focus. The NICE framework is a way to describe cybersecurity work. It provides common definitions and a taxonomy that describes seven categories, 33 specialty areas, and 52 work roles, and there's lots of details in the framework including, tasks, knowledge, skills and abilities. But it really helps to bring those work roles and specialty areas to light when we can profile somebody who's doing the real work. So, I'm pleased today to welcome Matthew McCollough, from Minnesota, who's going to talk to us about his work in cybersecurity. Matt, thanks for joining us today.

**Mr.** **McCollough**: Thank you for having me.

**Mr. Petersen**: Matt, why don't you explain a little bit about your role and responsibilities as a SOC analyst, a security operations center analyst.

**Mr.** **McCollough**: My role as SoC analyst kind of revolves around three primary responsibilities right now. The first one being, what we kind of "eyes-on glass", which is your serious, typical SOC duties of parsing through all of our logs, and looking through our SIMS, and trying to identify any actionable incidents, or actionable threats that are happening on our network. When we're not doing that, my other two roles revolve around two other kind of big projects we're rolling out at the State of Minnesota. The first one being, I manage the endpoint anti-virus solution for the 25,000endpoints we have. When that's not taking up the rest of my day, I help out with the third project which is we're trying to encompass all of our county networks into our centralized state network and helping roll out our daily IT solutions to each of them.

**Mr. Petersen**: Great, thank you Matt. Can you talk a little more about the size of the team and the security operations center and what type of roles do others fill?

**Mr.** **McCollough**: We have kind of a lean team of about 14 different analysts. We all are tasked with different "eyes on glass" daily incident work, kind of threat-casting for lack of a better word. But some of the other roles that are on our team are network architects, security architects, that are responsible for kind of the big picture, the defense and depth which kind of figuring where we're lacking in that. We've got a guy that's working specifically firewalls, we've got a couple of newer analysts that are kind of working on triaging events, and we've got a couple of people that are tasked with tuning our IPS/APS and our STEM and weeding out mountain of work that we get.

**Mr. Petersen**: Great. Sounds like a great combination of our "Protect and Defend" category, as well as "Analyze" category. Can you talk a little bit about your career path of becoming a SOC analyst?

**Mr.** **McCollough**: I took what I consider an unconventional path. I was originally in the medical field, and my original degree path was for the medical field. But I found that my real passion was there for computers, and I went straight in for a system admin degree. And from there, the instructor kind of pushed me into cybersecurity and then really opened my eyes to the world and how vast an area the world of cybersecurity is, and how much potential there is for really doing good, and helping, not only your business, but helping the country, and helping society just become more secure. And from there, I went for my two-year degree, finished up my four-year, and actually went on and did my master’s degree in cybersecurity as well.

**Mr. Petersen**: That's terrific. It's great to hear a non-traditional career pathway into a cybersecurity role. How would you envision using the NICE Cybersecurity Workforce Framework to further guide your career?

**Mr.** **McCollough**: I love how granular the framework gets down to the KSAs and how it breaks down each work role into certain KSAs really helps guide me if I have interest across multiple different categories and it will help guide me toward using those KSAs and saying hey, I want to learn more about forensics, and here's the work roles that I can fill in or, vice-versa I can look and see here are some positions that are open around me that are interesting and I can drill into the KSAs, and go, hey, this is what I need to become stronger in.

**Mr. Petersen**: What type of cybersecurity jobs are the most difficult for you to fill in the Minnesota IT organization?

**Mr.** **McCollough** Right now, we've got plenty of positions open for government risk and compliance, kind of policy that seem to be most in demand, at least the most frequent ones that are posted. Otherwise, we're definitely trying to grow at a rapid pace. So, it really comes down to anybody that's passionate about cybersecurity.

**Mr. Petersen**: How do you decide in your position description whether or not an academic degree or a cybersecurity certification is required?

**Mr.** **McCollough**: We kind of talk among the team that's looking to hire, and we lean on the team's experience and what kind of degrees and certifications they have, and what programs they've come out of and say, you know, is degree "x", or certification "x", really pertinent to what we do on a daily basis, or what we envision this role becoming on a daily basis? That's kind of how we nail down which degrees and certifications really are important to the role that we're posting.

**Mr. Petersen**: I wonder if Minnesota IT is doing anything to try to diversify its workforce or your description of how you sit around and talk about kind of what your similar backgrounds are. Are there any things you're looking to do to recruit a more diverse workforce that would round out your team's strengths and weaknesses?

**Mr.** **McCollough**: I know a lot of the team members, when there's a big push from our management to attend conferences, and help strengthen local schools and programs, by going out and helping out the cybersecurity crowd there, one of them was actually the women in cybersecurity. We've had a lot of members of our team go and speak on panels and give presentations at that specific program as well as the three-city program here in Minnesota that aims to help grow the interest across a diverse field of people.

**Mr. Petersen**: How do you keep your skills sharp and current?

**Mr.** **McCollough**: Being one of the more junior guys on the team, I love to ask as many questions as I can. I'm not really shy. If it's what I feel should be an obvious answer, typically those are the best questions, or best responses that I get from my senior analyst are those that are very obvious because it spurs more discussion on more advanced topics. And then, obviously, I just have a passion for learning new skills and learning new, or prepping, for new certifications and exams, just to keep up on what's new and happening in cybersecurity.

**Mr. Petersen**: A great way for practitioners to keep their skills sharp and learn is to give back either as a mentor, trainer, or an educator and I understand you're doing exactly that with one of your alma maters. Can you talk a little bit about what you're planning to do as an instructor?

**Mr.** **McCollough:** The original computer degree in network systems administration that I had, the lead instructor there reached out and asked me to teach the IDS and IPS course this year. I'm currently working on developing an up to date curriculum on IDS and IPS for a two-year degree, and really focusing on getting hands on experience for between some kind of integrating inside the whole. We have a module piece kind of education system, where students get hands-on experience that is directly equivalent to real world careers.

**Mr. Petersen**: That's great. Thanks for giving back and thanks for helping to connect students to the real world. What is it you enjoy most about the work you do as a SOC analyst?

**Mr.** **McCollough**: I think the thing I enjoy most is just the constant absolute need to learn. You have to always be open to learning new things and new ways of doing things because one week, threat actors can be doing one thing, and the next week they're doing a little different thing. You always need to be on top of what's new and what's a new method that comes out. Especially this time of year with BlackHat and DefCon coming out. It's a great time of year to learn about the new zero-days and methods that threat actors will be using throughout the year. And that just really interests me, and it doesn't hurt that also I'm tasked with defending an entire state network. It's a source of pride as well.

**Mr. Petersen**: That's great. If you could give advice to a young person considering a career in cybersecurity, what would you tell them?

**Mr.** **McCollough**: Find something, the biggest thing is just find something in the field of cybersecurity that you're passionate about in the field of cybersecurity because it is such a vast field. There are so many different things you can learn, and so many different paths you can go down. If you can find somebody, ask your instructor, ask the class ahead of you and say hey, you know, have you guys learned anything, and can I kind of come in under your wing and learn with you or help you with this project. Reach out. It's a great community of people that are very much all about sharing information and helping bring everybody up as a group to a higher level. A great field to be in and show up and be passionate about what you're doing because it will pay off a lot.

**Mr. Petersen**: We're talking with Matthew McCollough, the security operations, or SOC analyst, for Minnesota IT Services, and Matt, thank you so much for joining us today.

**Mr.** **McCollough**: Not a problem, and you guys have a good weekend.

**Mr. Petersen**: Thank you.